TRANSLATION

Title: Secure computer network with a network screen

Inventor: Vladimir S. Zaborovskiy
Correspondence:
Name and Address: Fractel Inc, 6748 Willow Grove Place Dublin, OH, 43017

FIELD OF THE INVENTION

The invention relates to a computer firewall.

BACKGROUND OF THE INVENTION

The majority of local computer networks (LCN) today have access to the Internet. However existing network protocols do not have special internal security features to secure private networks and keep data integrity. Therefore the inlargement of different features and increasing requirements to the network security demand usage of special devices to block selectively information resources and control data exchange between different computer networks.

Network screens are widely used as such devices called firewalls. A network screen is a special network device that is located between two different segments of an LCN in such a way that packets exchanged between these two segments is limited by special filter rules for incoming and outgoing data streams. Such a device may be installed between secured segment of an LCN and a router with one of its ports connected to the Internet. In that case filter rules of the packet traffic may block inbound and outbound activities of a secured LCN including given users, time of day, days of week and months.

An example of existing firewalls is US Patent No. 5,898,830, which is incorporated herein by reference, that represents a network screen located between two

computer networks with transparent network activity for the users of the secured network. For this purpose the network screen supports a configuration of two sets of virtual subscribers. The first set may be addressed only from secured segment and the second one may be addressed only from the opened segment of the network. These two sets are software compatible by the table adequacy of their network addresses as it is done for DNS servers. Provisioning and restriction for the data packets from a virtual subscriber with one set of addresses to the virtual subscriber with another set of addresses is done in accordance with the rules of packets filtration that are kept in the configuration file of the network screen.

Virtual subscribers, except one that is especially devoted to this purpose, do not have access to the system files and other system resources of the device used as a network screen. A control program module provides configuration of the network screen and, more particularly, creation of virtual users in accordance with the configuration files written when the device was started. Access to these configuration files can be provided using the rules of authorization function by a special virtual user addressed from the computer network. These rules include check of identity and authorization of the user that made a request. When this access is provided, the configuration file of the network screen that controls data exchange between computer networks may be modified. Transparency of this screen to the network level protocols does not mean that this network screen cannot be discovered using special software tools. Since a set of secured network units is screened by one network interface on the channel level of the network activity, each of these units is identified by the physical address of this network interface.

The procedure of identification of the network subscriber used to get access to the configuration file is not secured against intruders. That means the possibility of unauthorized access exists by trying different passwords or using hidden software holes.

SUMMARY OF THE INVENTION

The invention is a secure computer network with a network screen relates generally to security engineering in a telecommunication network, and, particularly to the hardware and software components of the network screens (firewalls) used to block unauthorized access and data exchange between different components of computer network.

The invention takes advantage of the capability of using the principle of the warranted security based on complete secretion of network interface addresses of a secured device. This task is resolved by using the network screen that has network interfaces for the data exchange between the network units but it does not have a network address. This network screen does not use network addresses for its functionality and it does not send physical addresses of the network interfaces to the external network. Therefore, this network screen cannot be located by any tools of secured or opened segments of the network.

According to the present invention, a special network screen is used to control filter processes of the packets traffic. This screen is completely isolated from the network interfaces that make it possible to avoid any possibility of unsanctioned access to this network screen for the users of secured and opened segments of LCN. The problem of warranted security is resolved also by the inability of users of opened or secured

segments of the network to create any special channel the packet data exchange between network interfaces and direct interface by means of internal system bus used for the special network screen. This special network screen keeps information about the addresses of sender and/or receiver using the rules of packet filtration that makes it possible to hide the existence of the network screen from users. In other words, the filter program excludes the network screen from the list of receivers of informational packets that are coming to the network interfaces while the network screen sends the packets only to external receivers.

BRIEF DESCRIPTION OF THE DRAWINGS

This and other advantages of the invention will be apparent those of ordinary skill in the art by reference to the following detailed description and the accompanying drawings.

FIG. 1 is a general view of the network screen from the front panel side where control units and interfaces of external connections are located.

FIG. 2 is a schematic illustration of the connection between two local computing networks connected also with external network via network screen

FIG. 3 is an adapted algorithm for the program of control information blocks transmission that are coming to one of the interfaces of the network screen.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In FIG.1 the network screen 1 used for the local computer network (LCN) is a special computer device with internal operational system. Such a computer device may

be based on personal computers motherboard (Gygabyte, GA-5AX) that may have up to 5 external devices connected with an internal PCI bus. Such a computer device may use different types of processors including Pentium MMX, Cyrix MII, AMD K-6, RISC MIPS and others. The network screen 1 contains network interfaces for packet data exchange such as Ethernet adapters of different types with 100 Mbit/sec for ISA OR 100/10 Mbit/sec for PCI bus; for example Fast Etherlink XL 3Com.

The front panel 2 of the network screen contains connectors for 3 data exchange interfaces, shown as reference numerals 3, 4 and 5. Each of the network adapters is connected to a local computer network segment build on the universal bus architecture with Ethernet protocol. The network screen may be used up to 5 segments of the LCN. If the LCN uses a different protocol its network adapters should support this protocol, too. The front panel 2 also contains connectors for 9 and 25 contacts for the interfaces 6 and 7 of COM ports using standard RS232C. One of these connectors is used as operational interface that modifies the program of control of the data exchange between segments of the LCN connected through network screen 1. The LCN segments may be connected to interfaces 3 or 4, or interfaces 3, 4 and 5 depending on their quantity. There is also a connector 8 and a source switch 9 on the panel 2. On this embodiment of the invention network screen 1 has operational system UNIX that provides multitask functionality for the program of control in accordance with configuration file that is located in source undependable memory device of the network screen 1.

In FIG.2 is shown an example of a connection between the LCN and the network screen 1. Network screen 1 there splits secured corporate LCN 10 with bus architecture into segments 11, 12 and 13 connected, respectively, to the network adapters 3, 4 and 5.

Such a structure of LCN 10 may be used in the corporate computer network where different network segments are used for different types of data applications. These applications may have different requirements for the level of confidentiality of delivered data that is taken into consideration for each of the network interfaces.

On this example segment 13 contains only one subscriber, gate 14, that provides connection of the LCN 10 with an external network 15. The network 15 may be connected with the other network also. The gate 14 can use modem lines to connect the LCN with the Internet using dial-up channels. Each of the segments 11 and 12 of the LCN contains several subscribers 16 and 17 that are connected to these network segments by the Ethernet adapter 18. To make changes in the program of control network packets delivery between interfaces 3, 4 and 5 including filter rules, a special computer 19 is connected to control interface 6. These modifications of the control program may be done from the computer 19 using a standard program of a Web navigator (browser), for example Netscape Navigator, using a connection between computer 19 and network screen 1 authorized with password by protocol PPP.

The program of control provides network packets delivery between the network interfaces that are addressed to the users of opened or secured segments. Since the network screen does not have addresses associated with its network interfaces, this screen cannot be used as a receiver of any network packets, it can be used only as a passive transit unit between network interfaces or as a breaker that rejects packets that did not pass filter rules between these interfaces. The program of control network packets delivery for interfaces 3, 4 and 5 (driver of the network adapters Ethernet) keeps

unchanged address filed of sender in their information blocks that are delivered to the network screen 1 through interfaces 3, 4 and 5.

The gate 14 works as a router that exchanges information about conditions of the network connections with another device of the same kind and sends packet traffic to the other segments of the corporate network and to the Internet. Therefore, the LCN 10 is completely secured by the network screen with network interfaces that do not have physical (MAC) and logical (IP) addresses. Such a screen is untouchable for remote attacks through computer networks because it is not a receiver of the information packets. The network screen cannot be detected by standard tools of network identification because its interfaces used for connections with network segments are operated in such a way that they do not answer for ARP requests about their physical (MAC) addresses.

FIG.3 shows an algorithm of filter packets coming to the network interface 5. Each packet coming through the segment 11 of LCN 10 receives by interfaces 5 that keep it in its buffer memory. Primary processing of it according to the filter rules consists of a sequential execution of the operations 20 and 21 that is a sequential test of receivers physical address Ad in the header of the processing packet.

What is claimed is:

1. A local computer network for packets delivery with headers that contain logical and physical addresses of senders and/or receivers of information and a network screen that splits it to at least two segments and represents a complex of hardware and

software means and contains at least two network interfaces for packets exchange between the network segments and a program that controls the process of packets commutation between the network interfaces based on the filtration rules that do not name logical addresses to the network interfaces and do not send their physical addresses to the net and at the same time permit a transit delivery through the network interfaces of the network screen only to the packets with the headers that passed the test in accordance to the defined filter rules and using a special direct interface to define these filter rules.

2. The invention of claim 1 wherein outbound packets keep in their headers physical addresses of the senders because the program that controls the network screen does not send outside local network physical addresses of its network interfaces.
3. The invention of claim 1 wherein the network screen is based on a universal computer device with operational system and several network interfaces and special direct interface where network interfaces are Ethernet adapters and special control interface may be based on Ethernet interface type or on the base of sequential asynchronous interface.
4. The invention of claim 1 wherein filter rules of the network screen disallow a transit delivery of any messages without special mark and address parameters in their headers.
5. The invention of claim 1 wherein the access to the program of editing filter rules is protected by password.
6. The invention of claim 1 wherein the network screen after processing the packet with filter rules keeps unchanged logical and physical addresses of the sender in the

packet's header and it does not name network interfaces with logical addresses and does not send their physical addresses to the network segments connected with them while the network screen contains special direct interface to edit and tune filter rules where any changes of filter parameters may be processed only through this interface and the program of control provides packet delivery from one network interface to another only when the information in the packet's header satisfies all filter requirements.

7. Network screen of claim 6 wherein this screen is a special computer device with internal operational system universal bus for data exchange between the interface adapters and a separate channel of control protected by password.

Abstract

This invention takes advantage of the capability to keep secured physical and logical addresses of the internal subscribers of the local network using a special network screen for the packets exchange between the network segments and using a special program to control the packets communication processes between the network interfaces. The program of control resolves the task of information delivery using special codes in the packet headers that are different from their logical and physical addresses. The network screen has a special interface to change, control and tune filter parameters.